

I claim:

1. A system for restoring a terminal to a default condition, comprising:

a random number generator included in the terminal; and

a file authentication arrangement for authenticating a clear file that includes a random number generated by said random number generator upon downloading of the clear file into the terminal.

2. A system as claimed in claim 1, wherein said file authentication arrangement includes a private key and a corresponding public key clear certificate containing information necessary to authenticate the clear file.

3. A system as claimed in claim 2, wherein said clear certificate contains information necessary to authenticate the clear file, said terminal being arranged to execute a clear instruction upon authentication of said clear file.

4. A system as claimed in claim 3, wherein said clear certificate is a sponsor public key certificate stored in the terminal and corresponding to a signer certificate downloaded with the digitally signed file,

said signer certificate corresponding to a private key used to digitally sign said clear file.

5. A system as claimed in claim 2, wherein said private key is stored on a smartcard and is only accessible by a secure processor embedded in the smartcard.
6. A system as claimed in claim 5, wherein said sponsor public key certificate is stored in a read only memory in said terminal.
7. A system as claimed in claim 2, further comprising a file signing tool for digitally signing said clear file, said file signing tool including a smartcard reader, and wherein all digital signing operations requiring access to said private key are carried out by a secure processor embedded in a smartcard inserted into said smartcard reader.
8. A system as claimed in claim 2, wherein said smartcard further has stored thereon a signer certificate for authenticating said digital signature, and wherein said clear certificate authenticates said signer certificate.



12. A method as claimed in claim 10, wherein the step of digitally signing the regular file comprises the steps of inserting a smartcard having an embedded secure processor in a smartcard reader connected to the file signing tool, causing the secure processor to access the private key in order to generate the digital signature.
13. A method as claimed in claim 12, wherein the step of authenticating the digital signature comprises the step of authenticating the digital signature based on a signer public key certificate downloaded into the terminal together with the signed clear file.
14. A method as claimed in claim 13, wherein the step of authenticating the digital signature further comprises the step of retrieving a sponsor public key certificate from a read only memory in said terminal and authenticating the signer certificate using the sponsor public key certificate.
15. A method as claimed in claim 13, wherein the step of authenticating the digital signature based on the signer public key certificate comprises the steps of comparing a value derived from the digital signature using the signer public key certificate with a value

derived from the stored random number to authenticate said clear file.

16. A method as claimed in claim 13, wherein the step of restoring said terminal to a default condition comprises the step of reading a clear string in a file type field of said signer public key certificate.
17. A method as claimed in claim 10, wherein said step of restoring said terminal to a default condition comprises the step of deleting a certificate tree from said terminal.